THE USE OF RENEWABLE AND DISTRIBUTED TECHNOLOGIES TO IMPROVE ENERGY SECURITY ON MILITARY FACILITIES

Bill Black
(bdblack@sandia.gov)

Presented by
Abbas Akhil
(aaakhil@sandia.gov)

Sandia National Laboratories
Albuquerque, NM

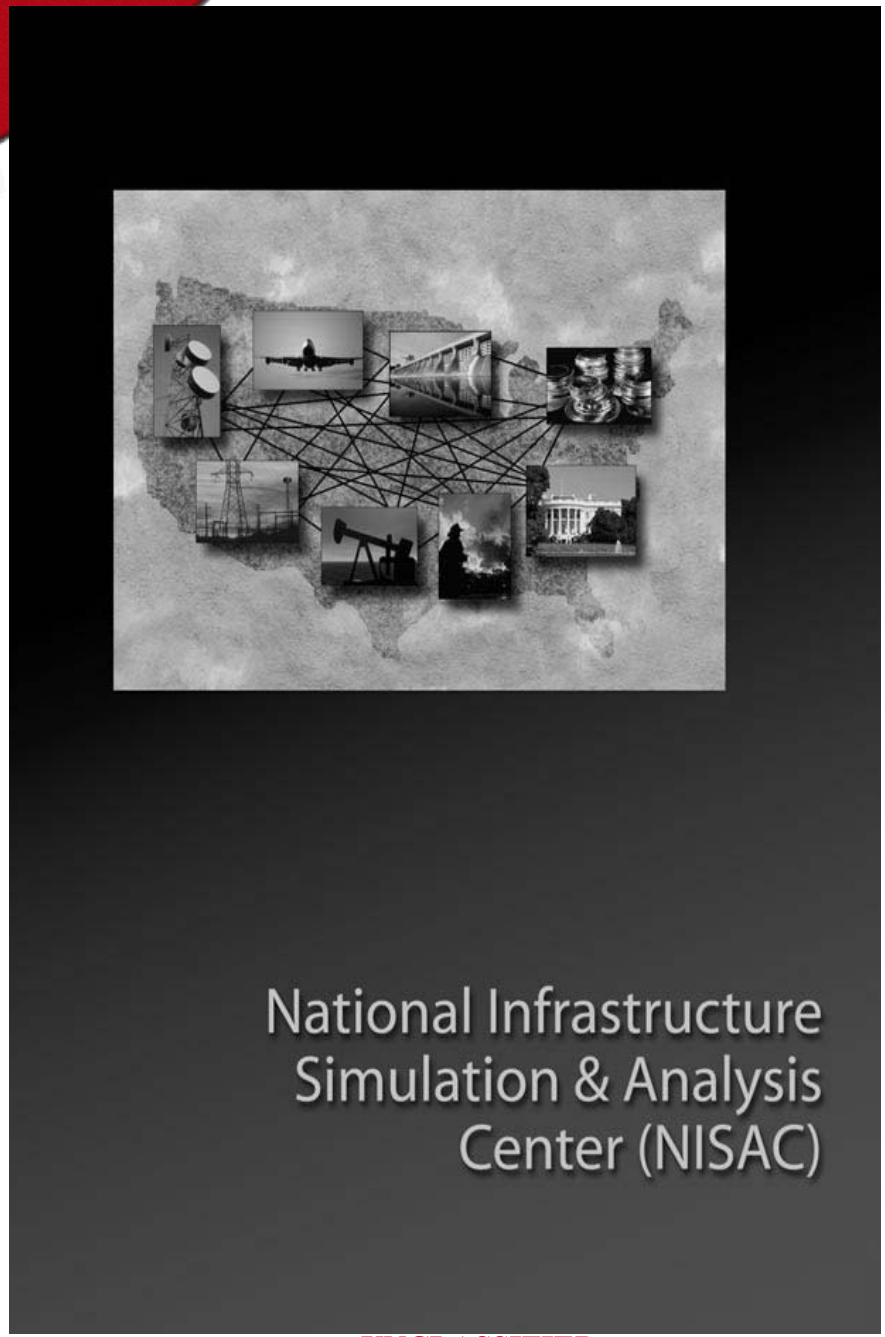
Presentation Outline

1. Overview of Sandia National Laboratories
2. Review of energy security-related issues
3. Basic energy security concepts and generic examples
4. Role of distributed and renewable energy technologies
5. Distributed and renewable technologies for energy reduction
6. Summary

Some Background on Sandia Laboratories

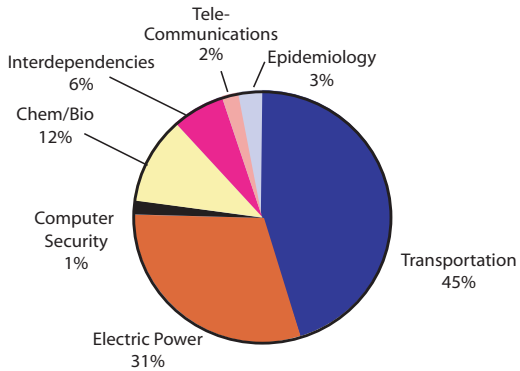
- Largest DOE National Lab, 8000 staff; $1.4B
- Multi-program, systems engineering lab with defense emphasis
- Work in renewable energy for 25 years—longer than any other lab

- Several test labs in renewable and distributed energy resources
- Security issues are among Sandia's core competencies
  - Sandia/LANL recently funded to develop the National Infrastructure Simulation and Analysis Center
  - Sandia is currently working with two bases on security and renewables project

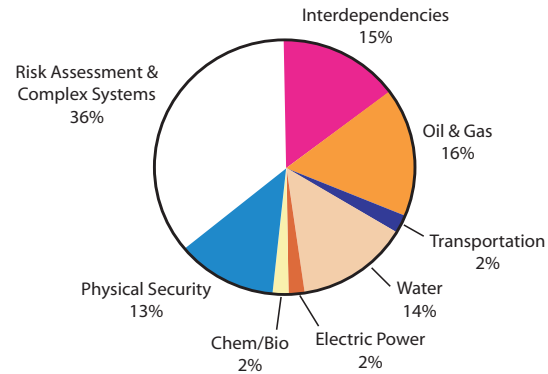

National Infrastructure
Simulation & Analysis
Center (NISAC)

The charts below illustrate the budget allocation that both Los Alamos and Sandia have attributed to modeling and simulation in the Critical Infrastructure area.

Infrastructure Modeling and Simulation Funding at LANL $80 Million



Infrastructure Modeling and Simulation Funding at SNL $80 Million



Summary

Utilizing the broad science base, simulation capabilities, and analysis expertise resident at SNL and LANL, The National Infrastructure Simulation and Analysis Center (NISAC) will provide critical support to government and industry decision makers in infrastructure issues to improve the national security and quality of life of the United States.

Field Manuals for Risk Assessment Have Been Developed and Validated

- Presidential Decision Directive 63, Protecting America's Critical Infrastructures (PDD 63), May 98
- Adaptation of risk assessment processes for the protection of nuclear weapons and other nuclear materials.
- Risk Assessment Methodology for Electric Power Transmission, Feb 02
- Risk Assessment Methodology for Dams
- Risk Assessment Methodology for Chemical Plants
- Risk Assessment Methodology for Municipal Water Systems

This cover sheet is not proprietary or official use only

PROPRIETARY INFORMATION










Risk Assessment Methodology for Electric Power Transmission (RAM-T^{SM})

FIELD MANUAL

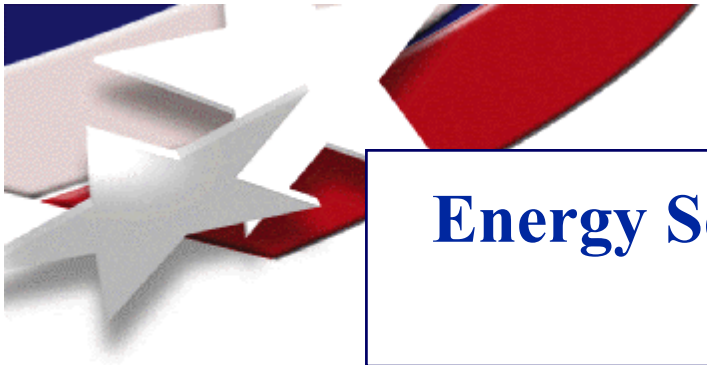
Prepared by
Sandia National Laboratories

OFFICIAL USE ONLY
Contains information which may be exempt from public release under the Freedom of Information Act (5 USC 552), exemption numbers (s) 1. Approval by the Department of Energy Departmental Element prior to public release is required.

Originator: R. V. Matalucci Date: February 28, 2002
Further dissemination authorized to U.S. Government agencies and their contractors; other requests shall be approved by the originating facility or high DOE programmatic authority.

February 2002

OFFICIAL USE ONLY



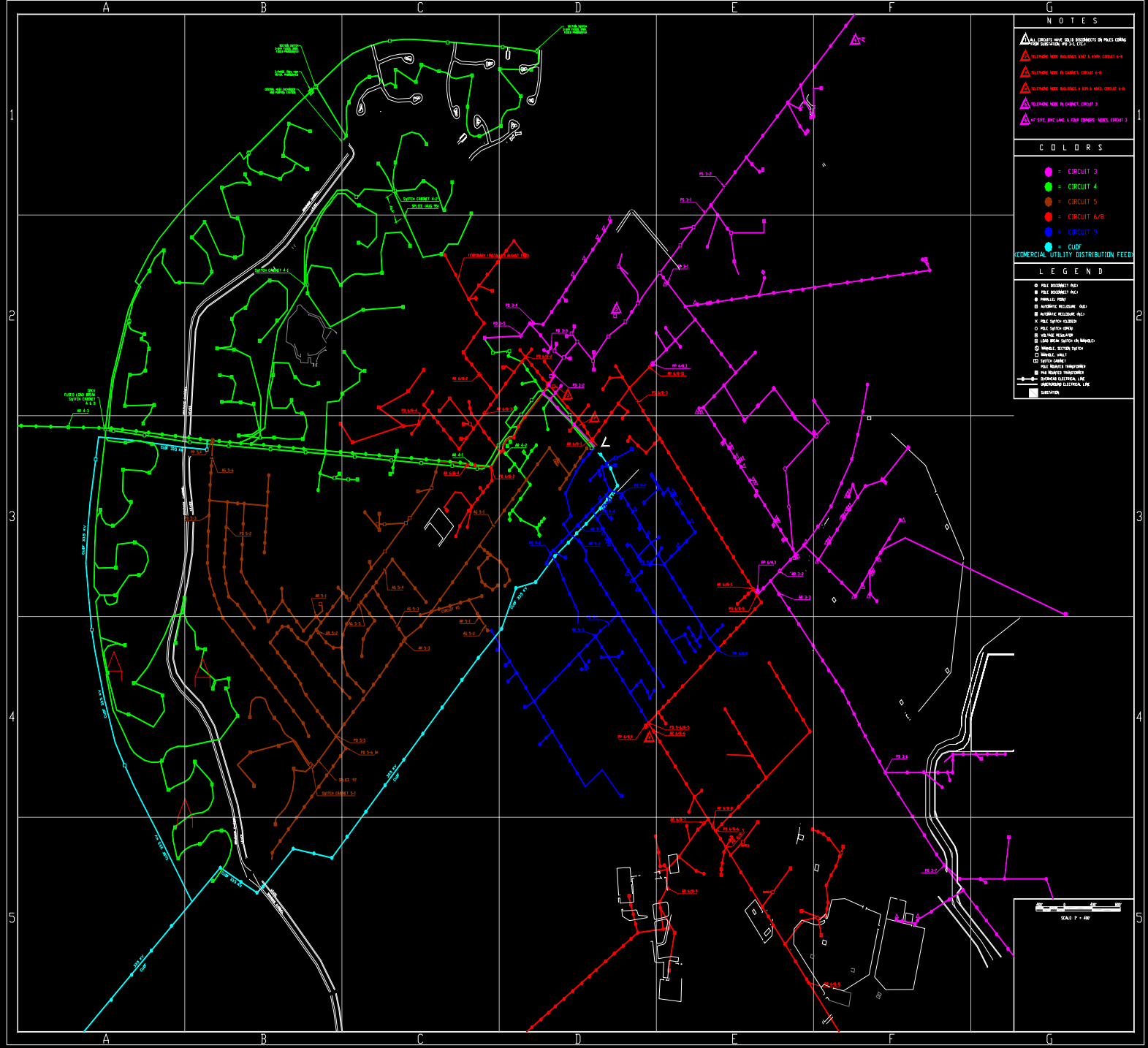
Energy Security Analysis Has Strategic Value

- Energy systems are critical infrastructure components of military bases
  - Electricity and gas; inter-dependencies with water; command and control
  - Energy infrastructures presently offer easy targets – from simply annoying to severely impacting mission critical activities
  - Must be given high priority for protection
- Security analysis reveals vulnerabilities that could be exploited by terrorists
  - Analysis must be conducted in an appropriately secure facility by cleared personnel
    - Sandia conducts its work in a Top Secret (Q) or Secret (L) environment

No classified information presented in this talk.

Only generic information is discussed with no specific details.

More information can be provided to cleared individuals with a need-to-know.

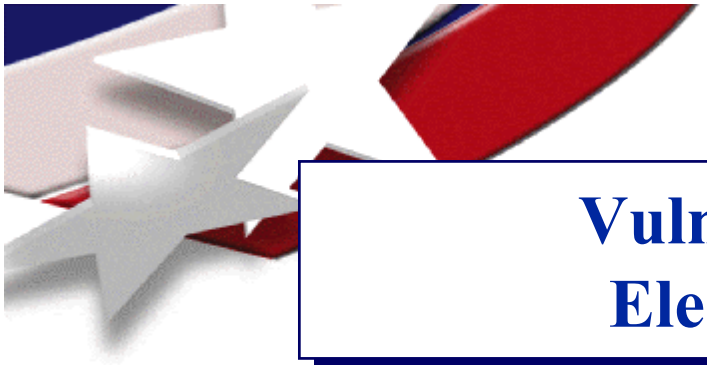

NOTES
ALL CIRCUITS HAVE SOLID DISCONNECTS ON POLES COMING FROM SUBSTATION, #'S 3-1, ETC.
TELEPHONE WORK BUILDINGS #247 & #249, CIRCUIT 6-8
TELEPHONE WORK IN CABINET, CIRCUIT 6-8
TELEPHONE WORK BUILDINGS # 839 & #843, CIRCUIT 6-8
TELEPHONE WORK IN CABINET, CIRCUIT 3
AT SITE, BIKE LANE, & FOUR CORNERS WORKS, CIRCUIT 3
COLORS
= CIRCUIT 3
= CIRCUIT 4
= CIRCUIT 5
= CIRCUIT 6/8
= CIRCUIT 9
= CUDF
COMERCIAL UTILITY DISTRIBUTION FEED
LEGEND
POLE DISCONNECT (NO)
POLE DISCONNECT (NC)
PARALLEL POINT
AUTOMATIC RECLOSURE (NO)
AUTOMATIC RECLOSURE (NC)
POLE SWITCH CLOSED
POLE SWITCH OPEN
VOLTAGE REGULATOR
LOAD BREAK SWITCH (IN MANHOLE)
MANHOLE, SECTION SWITCH
MANHOLE, VAULT
SWITCH CABINET
POLE MOUNTED TRANSFORMER
PAD MOUNTED TRANSFORMER
OVERHEAD ELECTRICAL LINE
UNDERGROUND ELECTRICAL LINE
SUBSTATION
SCALE 1" = 400'
A
B
C
D
E
F
G
1
2
3
4
5

Brush Fire Takes Down Fort Huachuca, AZ for 16 Hours

- Fort Huachuca is served by Tucson Electric Power, 138kV line and 46kV backup line , 30 April 2002.
- **11:00** Ryan brush fire is 3.5 miles from 46kV backup line.
- **13:00** 46 kV line voluntarily de-energized, fire continues toward 138kV
- **15:00** Fire reaches 138kV line but it is still in service.
- **23:50** Fort Huachuca is **Dark**. 138kV line out of service.
- **06:30** 12 poles damaged on 46kV, one 2-pole structure down and numerous others damaged on 138kV line.
- **10:30** Fire flares up again, crews evacuated
- **15:50** Fort is 100% on-line, 16 hours later

Vulnerability of Off-base Electric Infrastructure

- Off-base facilities and information owned by electric utilities
  - Substations, switchyards, poles, cables
  - One-line diagrams, maps, access and control of key facilities
  - **Controlling this access and information off-base may not be practical or enforceable**
- Sample vulnerabilities
  - Single feeder to base – poles and conductor easily taken out with low probability of detection
    - Line restoration could exceed several days
  - Substation transformers and hardware – disabled with readily available tools such as a rifle or a hand drill
    - Transformers, breakers and other hardware are long-lead time items – spares are not usually stocked by the utility
    - Outage could last several months depending on spares availability



Vulnerability of On-base Electric Infrastructure

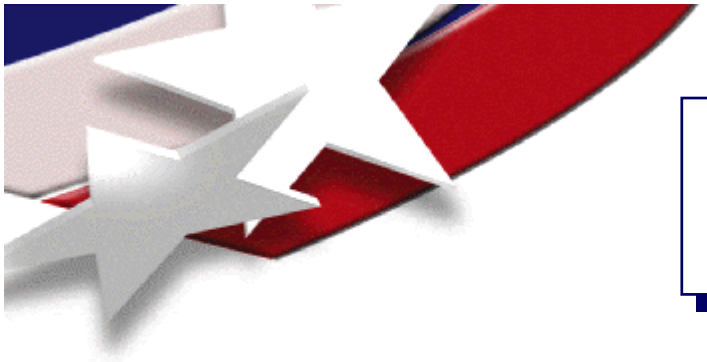
- Unlike off-base facilities, controlling information and access to on-base facilities is achievable
- On-base electric infrastructure elements are basically similar
  - Substations, switchyards, poles, cables
  - Except on-site and stand-by generators, physical plant and special use facilities and fuel storage bunkers
- Protection needed includes controlling physical access, camouflaging thermal and noise signatures
- Typical vulnerabilities
  - Sabotaging substation, stand-by generation and UPS equipment
  - Coordinated outages programmed through building energy management systems

Simple Terrorist Attack Strategy

- Use low-tech tools and low profile approach

- Cut the utility feeder line to base
  - Approach: Spot key structural poles and shoot conductor and insulators
  - Tools: .30-06 rifle with scope, ordinary ammo; one horse or ATV optional
  - Damage: Possible base-wide outage of 1 – 3 days while line is rebuilt

- Disable key substation transformer(s) – On or Off-base
  - Approach: Break into substation and loosen transformer oil drain plug
  - Tools: Padlock cutter, hex wrench
  - Damage: Burnt transformers; replacement takes 3 – 6 months based on transformer size and availability; base power supply curtailed or severely limited for extended time period.



Coordinated Terrorist Attack Strategy

- Disable critical staging bases
- Then follow-on attack at principal location

How Can Distributed and Renewable Sources Increase Energy Security

- Distributed resources are inherently dispersed and represent incrementally small power blocks
  - Less threat exposure than centralized generation
  - Distributed resources can be mobile
  - Size ranges from 10 kW to 3 MW
  - Mobility decreases threat risk
    - Generator location changes unexpectedly and frequently

Different Integration Approach for Distributed Energy

- Pre-plan and build supporting infrastructure to respond in event of attack
- Identify and prepare several "nodes" where (mobile) distributed generation could be tied in quickly
  - Sectionalize distribution as necessary to isolate and serve critical loads/facilities
  - Fuel source availability – supply or storage
  - Move switchgear underground or tightly integrate in building design
  - Reduce thermal and noise signatures

Our Understanding of DoD's Current Approach to Base Energy Security

- Identify vulnerabilities (i.e., specific sites on the base that could be natural disaster or terrorism targets)
- Design backup systems to provide power to those sites using UPS/diesel generators in case of attack. That is, distribute the backup power generation.
- Design facility and power system safeguards to minimize the probability of an attack
- Analyze impact of an attack to related infrastructure (transportation, water, communications, etc.) and plan contingencies

If that Operational Assumption is True, These are the Potential Problems

1) Some specific vulnerabilities may not have been identified in the post 9/11 threat scenario and backup systems may not be installed.

2) The backup systems are not normally operated and may not operate when required.

3) Maintenance is still required for backup systems that produce no revenue or savings.

4) Maintenance for backup systems may be minimal.

Our Current Concept of Using DER for Base Energy Security

- Identify vulnerabilities (i.e., specific areas on the base that contain potential terrorism targets)
- Prioritize the vulnerabilities from a power distribution point of view; identify the regions on the base that require protection and how much
- Design primary, on-site generation to provide power to critical regions on a **continuous** basis. That is, distribute the primary power generation.
- Analyze impact of an attack to related infrastructure (transportation, water, communications, etc.) and plan contingencies

Potential Advantages of Sandia's Concept to Base Energy Security

1) The primary generation is dispersed on the base making a destabilizing attack unlikely

2) The generation would cover a region of the base instead of a specific facility to minimize the impact of an oversight

3) Potential energy generation system failures resulting from an attack would be minimized because they normally operate full time

4) **Could save money on energy** over the long term by providing combined heat and power. (microturbine CHP 74-86% efficient)

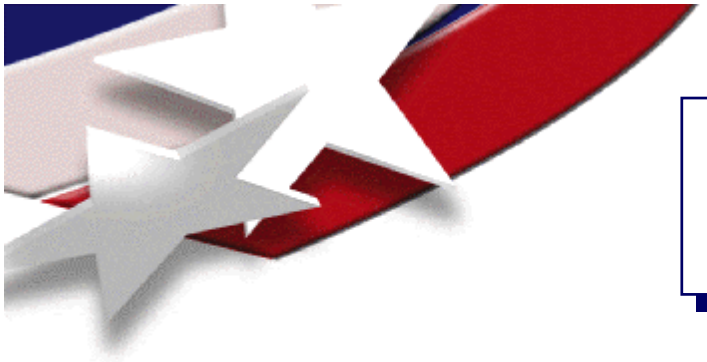
5) Maintenance would be applied to continuously operating systems rather than non-operating backups

Risk Reduction for Critical Loads e.g. Communication Center

- UPS
  - Provides fast response, short duration
  - Allows distributed resource time to come on-line
- Distributed Resource
  - Needs time to come on-line in stand alone mode
  - Diesel, startup time
  - Microturbine, time to switch from grid connect to stand alone, (7 min.)
- Can be used for single facility or micro-grid system approach

Attributes of DER

- Incremental capacity
- Mobility
- Camouflage - visual, thermal and noise signatures
- Fuel diversity
- Point-of-use location
- Environmental benefits



The National Energy Policy

- DER is a ***key component*** of the National Energy Policy…
- Of 105 total recommendations, ***21 affect DER***

"Renewable and alternative energy technologies, such as wind energy and combined heat and power could be significantly expanded, given today's technologies."

"Combined heat and power in buildings offers great potential for increased system efficiencies and lower costs."

Executive Order 13123

Greening the Government Through Efficient Energy Management

- **Sec. 201. Greenhouse Gases Reduction Goal.** Through life-cycle cost-effective energy measures, each agency shall reduce its greenhouse gas emissions attributed to facility energy use by 30 percent by 2010 compared to such emissions levels in 1990.
- **Sec. 202. Energy Efficiency Improvement Goals.** Through life-cycle cost-effective measures, each agency shall reduce energy consumption per gross square foot of its facilities by 30 percent by 2005 and 35 percent by 2010 relative to 1985.
- **Sec. 204. Renewable Energy.** Each agency shall strive to expand the use of renewable energy within its facilities and in its activities by implementing renewable energy projects and by purchasing electricity from renewable energy sources. In support of the Million Solar Roofs initiative, the Federal Government shall strive to install 2,000 solar energy systems at Federal facilities by the end of 2000, and 20,000 solar energy systems at Federal facilities by 2010.
- **Sec. 205. Petroleum.** Through life-cycle cost-effective measures, each agency shall reduce the use of petroleum within its facilities.
- **Sec. 206. Source Energy.** The Federal Government shall strive to reduce total energy use and associated greenhouse gas and other air emissions, as measured at the source. To that end, agencies shall undertake life-cycle cost-effective projects in which source energy decreases, even if site energy use increases. → Makes CHP a viable method for meeting EO energy reduction requirements
- FEMP is tasked with assisting Federal agencies in meeting these goals.

Summary

- Energy security analysis must be performed in an appropriate controlled environment.
- Military bases are increasingly conscious of energy infrastructure vulnerabilities. RE and DER could be a key element of the solutions portfolio.
- Off-base and on-base electric infrastructures share similarities but vulnerabilities differ.
- RE and DER can play a key role in enhancing survivability and operational continuity under severe threat conditions – natural disaster or attack.
- RE and DER can operate full time help meet energy reduction directives.